Nos. 23-2234(L) & 23-2241

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

HANAN ELATR KHASHOGGI,

Plaintiff-Appellant/Cross-Appellee,

v.

NSO GROUP TECHNOLOGIES LIMITED;
Q CYBER TECHNOLOGIES LIMITED

Defendants-Appellees/Cross-Appellants.

On Appeals from the United States District Court
for the Eastern District of Virginia
Case No. 1:23-cv-00779, Hon. Leonie M. Brinkema

BRIEF FOR APPELLANT

Michael J. Pendell
MOTLEY RICE LLC
One Corporate Center
20 Church Street, 17th Floor
Hartford, CT 06103
(860) 882-1681
mpendell@motleyrice.com

Michael J. Quirk
MOTLEY RICE LLC
40 West Evergreen Avenue,
Suite 104
Philadelphia, PA 19118-3324
(610) 579-9932
mquirk@motleyrice.com

Counsel for Plaintiff-Appellant/Cross-Appellee

April 1, 2024

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by all parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

Nos. 23-2234(L) & 23-2241
Caption: Hanan Elatr Khashoggi v. NSO Grp. Techn. et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Hanan Elatr Khashoggi
(name of party/amicus)

who is Appellant/Cross-Appellee, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a public held corporation or other publicly held entity? NO

2. Does party/amicus have any parent corporations? NO

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? NO

4. Is there any publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? NO

5. Is party a trade association? NO

6. Does this case arise out of a bankruptcy proceeding? NO

7. Is this a criminal case in which there was an organizational victim? NO

Signature: /s/ *Michael J. Quirk* Date: April 1, 2024

Counsel for: Appellant/Cross-Appellee Hanan Elatr Khashoggi

TABLE OF CONTENTS

DISCLOSURE STATEMENT ii

TABLE OF AUTHORITIES vi

INTRODUCTION 1

JURISDICTIONAL STATEMENT 3

STATEMENT OF THE ISSUE 4

PERTINENT STATUTES 4

STATEMENT OF THE CASE 5

A. Statement of Facts 5

B. Procedural History 11

SUMMARY OF ARGUMENT 16

STANDARD OF REVIEW 19

ARGUMENT 20

I. Virginia's Long-Arm Statute Covers Plaintiff's Claims. 20

II. Plaintiff Satisfies the Constitutional Requirements for Specific Personal Jurisdiction. 21

A. Defendants Purposefully Committed Acts in Virginia. 23

B. Plaintiff's Claims Relate Directly to Defendants' Acts in Virginia. 30

C. This Exercise of Personal Jurisdiction is Constitutionally Reasonable 33

CONCLUSION 36

REQUEST FOR ORAL ARGUMENT 36

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT.....38

CERTIFICATE OF SERVICE 40

TABLE OF AUTHORITIES

Cases

ALS Scan, Inc. v. Digital Service Consultants, Inc.,
293 F.3d 707 (4th Cir. 2002) 24-25

Automobili Lamborghini S.P.A. v. Lamborghini Latino Am. USA,
400 F. Supp. 3d 471 (E.D. Va. 2019) 25

Bristol-Myers Squibb Co. v. Superior Ct. of Cal.,
582 U.S. 255 (2017) 21-22, 23, 30

Burger King Corp. v. Rudzewicz,
471 U.S. 462 (1985) 24, 34

Butters v. Vance Int'l, Inc.,
225 F.3d 462 (4th Cir. 2000) 13

Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc.,
334 F.3d 390 (4th Cir. 2003) 24

Combs v. Bakker,
886 F.2d 673 (4th Cir. 1989) 19

Consulting Eng'rs Corp. v. Geometric Ltd.,
561 F.3d 273 (4th Cir. 2009) 14, 15, 23, 33-34

Daimler AG v. Bauman,
571 U.S. 117 (2014) 30

Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.,
592 U.S. 351 (2021) 21-22, 23, 24, 30

Goodyear Dunlop Tires Operations, S.A. v. Brown,
564 U.S. 915 (2011) 22

Grayson v. Anderson,
816 F.3d 262 (4th Cir. 2016) 19

Hanson v. Denckla,
357 U.S. 235 (1958) 22

Harris Rutsky & Co. Ins. Servs., Inc. v. Bell & Clements Ltd.,
328 F.3d 1122 (9th Cir. 2003) 34

Int'l Shoe Co. v. Washington,
326 U.S. 310 (1945) 21, 30

Keeton v. Hustler Magazine, Inc.,
465 U.S. 770 (1984) 24

Luis v. Zang,
833 F.3d 619 (6th Cir. 2016).....3, 17-18, 28, 29, 32-33

McGee v. Int'l Life Ins. Co.,
355 U.S. 220 (1957) 24

Popa v. Harriet Carter Gifts, Inc.,
52 F.4th 121 (3d Cir. 2022)..... 3, 27-28

St. Jarre v. Heidelberger Druckmaschinen, A.G.,
19 F.3d 1430 (4th Cir. Mar. 25, 1994) (unpub.) 33

Stover v. O'Connell Assocs., Inc.,
84 F.3d 132 (4th Cir. 1996).....21

UMG Recordings, Inc. v. Kurbanov,
963 F.3d 344 (4th Cir. 2020)..... 19, 26

Velasco v. Gov't of Indonesia,
370 F.3d 398, 399 (4th Cir. 2004) 13

WhatsApp Inc. v. NSO Group Techs. Ltd.,
17 F.4th 930 (9th Cir. 2021) 13

WhatsApp Inc. v. NSO Group Techs. Ltd.,
472 F. Supp. 3d 649 (N.D. Cal. 2020) 35

Young v. New Haven Advocate,
315 F.3d 256 (4th Cir. 2002)..... 20, 21

Statutes

18 U.S.C. § 1030 .....3, 11

28 U.S.C. § 1291 3

28 U.S.C. § 1331 3

28 U.S.C. § 1367(a) 3

28 U.S.C. § 1603(a) 13

Va. Code Ann. § 18.2-152.1 *et seq*. (2023) 11

Va. Code Ann. § 8.01-328.1(A)(3) (2023) 4, 16, 20

Va. Code Ann. § 8.01-330 (2023)..... 4, 16, 21

Rules

Fed. R. App. P. 28(f).....4

Fed. R. Civ. P. 12(b)(2)..... 13, 19

Fed. R. Civ. P. 12(b)(6).....12

Regulations

Addition of Certain Entities to the Entity List,
86 Fed. Reg. 60759 (Nov. 4, 2021) (codified at 15 C.F.R. § 744) 11

Other Authorities

2019 ISS World Europe -Lead Sponsor,
TeleStrategies ISS World Europe
[https://web.archive.org/web/20190908051829/https://www.issworldtraining.com/iss_europe/sponsors.html] (last visited Mar. 29, 2024)..... 26-27

Aishvayra Kavi, *Widow of Jamal Khashoggi Is Granted Political Asylum in the U.S.*, N.Y. Times (Dec. 21, 2023), https://nytimes.com/2023/12/21/us/politics/jamal-khashoggi-widow-asylum.html 5

Ronan Farrow, *How Democracies Spy on their Citizens*, The New Yorker (April 18, 2022), https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens 9, 10, 26

INTRODUCTION

Plaintiff Hanan Elatr Khashoggi ("Plaintiff" or "Hanan") is the widow of the late journalist and activist Jamal Khashoggi. She has lived in Virginia since she and Jamal were married there in June 2018. In October 2018, four months after their wedding, Hanan found out with the rest of the world that Jamal had been brutally assassinated and dismembered while visiting the Saudi Arabian Consulate in Istanbul. United States intelligence authorities concluded that the Saudi Arabian government had approved and orchestrated Jamal's assassination.

Hanan later learned from a technology and human rights watchdog's examination that her Android smartphones had been infected with sophisticated surveillance software since before she and Jamal were married. This spyware system, "Pegasus," was manufactured and operated by Defendants NSO Group Technologies Limited and its parent company Q Cyber Technologies Limited, which are incorporated and headquartered in Israel. Pegasus captures every piece of data on a target's device, activates the device's microphones, cameras, and GPS without the target's knowledge, and collects information from the device in real time and in perpetuity. For Hanan, this meant that Defendants and their client—the United Arab Emirates—had accessed and obtained private and sensitive information about her finances, medical care, and—most alarmingly—her relationship with Jamal and information about his location and plans.

Defendants NSO Group and Q Cyber play an integral role in operating Pegasus for their clients. Defendants access the target's devices, extract the communications and data from the devices ("we can fairly easily extract the important data from virtually any application upon customer demand" (JA67)), and reroute this information through their "anonymizing network" to prevent detection and through their servers to the client's workstation.

Hanan brought this action alleging that Defendants violated federal and Virginia statutes and common law by intentionally accessing her devices and obtaining her information without authorization. Defendants moved to dismiss for, *inter alia*, lack of subject-matter jurisdiction based on derivative sovereign immunity and lack of personal jurisdiction. The district court rejected sovereign immunity, but granted dismissal for lack of personal jurisdiction, holding that Hanan did not adequately allege that Defendants committed acts in Virginia.

This ruling was in error. Defendants acted in Virginia by accessing Hanan's devices there, obtaining her communications and data, and rerouting this information through their anonymizing network and server to their client. The unlawful capture of electronic information occurs where a party accesses and reroutes it, which here was on Hanan's devices in Virginia. In holding that Defendants did not act in Virginia, the district court ignored Hanan's allegations and evidence placing herself in Virginia after she married Jamal and Defendants in

Virginia when they accessed and rerouted the information from her devices. A spyware operator's unauthorized interception is tortious conduct that occurs at the point of access. *See, e.g.*, *Luis v. Zang*, 833 F.3d 619, 633 (6th Cir. 2016); *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 130-32 (3d Cir. 2022).

These errors as to Defendants' acts in Virginia pervaded the district court's personal jurisdiction analysis. In holding that Hanan's claims did not relate to Defendants' forum contacts, the court again held that she did not adequately allege that she was in Virginia or that Defendants surveilled her phones. Similarly, in holding that exercise of personal jurisdiction was constitutionally unreasonable, the court weighed in the balance "plaintiff's inability to plausibly demonstrate that NSO Group directed its alleged conduct at her in Virginia[.]" JA202.

These errors pervading the district court's analysis compel reversal.

JURISDICTIONAL STATEMENT

The district court had subject-matter jurisdiction under 28 U.S.C. §§ 1331 and 1367(a) because Plaintiff asserts a claim under federal law, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and state-law claims that arise from a common nucleus of operative fact. JA38-44.

This Court has jurisdiction over Plaintiff's appeal under 28 U.S.C. § 1291. The district court entered final judgment on October 26, 2023. JA206. Plaintiff timely filed a notice of appeal on November 21, 2023. JA207.

STATEMENT OF THE ISSUE

Whether the U.S. District Court for the Eastern District of Virginia erred in holding that it lacked personal jurisdiction where Plaintiff, who resided in Virginia, alleges that Defendants, both foreign companies, intentionally and without authorization accessed her smartphones in Virginia, obtained the communications and data from her phones, and rerouted this information through their own anonymizing network and servers to a third-party foreign client.

PERTINENT STATUTES

Pursuant to Fed. R. App. P. 28(f), the following statutes are pertinent to the issues presented herein:

Va. Code Ann. § 8.01-328.1(A)(3) (2023): When personal jurisdiction over person may be exercised

> **A.** A court may exercise personal jurisdiction over a person, who acts directly or by an agent, as to a cause of action arising from the person's:
>
> . . .
>
> 3. Causing tortious injury by an act or omission in this Commonwealth[.]

Va. Code Ann. § 8.01-330 (2023): Jurisdiction on any other basis authorized

> A court of this State may exercise jurisdiction on any other basis authorized by law.

STATEMENT OF THE CASE

A. Statement of Facts

Hanan Elatr Khashoggi is a citizen of Egypt and a lawful resident of the United States. JA9. Hanan sought and now has obtained political asylum in the United States. JA9.[1] Hanan's husband, Jamal Khashoggi, was a prominent Saudi Arabian writer, editor, and activist who advocated for the rights of women and minority populations and for government reform in Saudi Arabia and the Middle East as a whole. JA9; JA26-28. Hanan met Jamal in 2009 at a conference in the United Arab Emirates ("UAE"). JA10; JA28. They became friends and stayed in touch by phone for years thereafter. JA28.

In late 2016, Jamal delivered a speech at the Washington Institute for Near East Policy that was critical of the incoming presidential administration in the United States. JA28-29. The government of Saudi Arabia then placed Jamal under house arrest. JA28-29. In June 2017, the Saudi government lifted Jamal's house arrest and allowed him to travel to the UAE to attend a conference. JA29. When he arrived at the Abu Dhabi airport, UAE authorities denied him entry. JA29. Sensing that he may be in danger, Jamal made the difficult decision to flee Saudi

[1] Hanan obtained political asylum in the United States while this appeal has been pending. *See* Aishvayra Kavi, *Widow of Jamal Khashoggi Is Granted Political Asylum in the U.S.*, N.Y. Times (Dec. 21, 2023), https://nytimes.com/2023/12/21/us/politics/jamal-khashoggi-widow-asylum.html.

Arabia. JA29. He sought refuge and obtained admission into the United States in the summer of 2017 and took up residence in Virginia. JA29.

At this time, and for over 20 years prior, Hanan was employed as a flight attendant for Emirates Airlines. JA10. After Jamal moved to the United States, he and Hanan began spending time together at and near his home in Virginia. JA10. Over the next year, their friendship developed into partnership, and in April 2018 they were engaged to be married. JA10.

Later that month, Hanan's work as a flight attendant brought her back to the UAE. JA31. There, at the Dubai International Airport, she encountered seven Emirati intelligence officers who blindfolded, handcuffed, and detained her. JA31. The UAE officers confiscated Hanan's cell phones and questioned her about Jamal for over seventeen hours. JA31. They then placed her under house arrest and detained her until late May 2018. JA31.

Upon her release, Hanan returned to the United States and to Jamal in Virginia. JA31. On June 2, 2018, the couple were married in Virginia. JA32. As wife and husband, Hanan and Jamal settled into their home in Tysons Corner, Virginia. JA10, JA32, where they both lived for the remainder of Jamal's life.

When work travel forced them apart, Hanan and Jamal kept in frequent contact through phone calls, text messages, WhatsApp, and other apps. JA32. In September 2018, Hanan and Jamal discussed their future plan of one day together

establishing a second home in Turkey, where Jamal was headed for a planned trip. JA33. This was the last time they were together. JA33.

Hanan soon found out with the rest of the world that Jamal would not be returning. On October 2, 2018, Jamal disappeared after entering the Saudi Arabian consulate in Istanbul. JA34. As days and weeks passed, reports emerged that Jamal had been assassinated and that his body was gruesomely dismembered. JA34. United States intelligence authorities concluded that the Saudi Arabian government approved and orchestrated the operation to assassinate Jamal. JA35.

Some three years later, Hanan learned that her personal devices had been infected with sophisticated surveillance software since 2017 or 2018. JA15-16. This spyware system, "Pegasus," is the "the world's most powerful cyberweapon" and the brainchild of Defendant NSO Group Technologies Limited ("NSO Group") and its parent company, Defendant Q Cyber Technologies Limited ("Q Cyber"). JA8, JA15. Defendants' Pegasus technology leads the spyware market because it collects "the most accurate and complete intelligence." JA56. Pegasus uniquely enabled Defendants to capture "every piece of data stored" on a target's device, activate the device's cameras, microphones, and GPS without the user's knowledge, and collect phone calls, text messages, and other communications in perpetuity. JA15-16, JA63-67. For Hanan, this meant that Defendants and their client—the UAE—had accessed and obtained sensitive, private information about

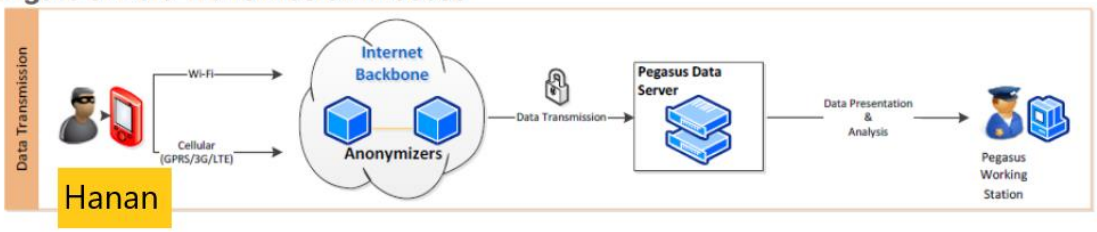
her finances, medical care, and—most alarmingly—her relationship with Jamal and information about his location and travel plans. JA15, JA37.

Defendants market, sell, operate, maintain, and update the Pegasus spyware technology, servicing their government clients and leveraging Pegasus towards myriad—sometimes despotic—ends. JA8, JA11, JA15, JA23-26. The software (called the "Agent") that is installed on a target's device is just one component of the "Pegasus system," which is a complex infrastructure of tools and services that Defendants operate and maintain for their clients. *See* JA57-59. At the outset, Defendants outline various agent installation methods that they can customize to a client's needs, including use of "Enhanced Social Engineering Message[s]," (a.k.a. "ESEM"). JA18, JA22, JA59-62. Defendants give clients pursuing the ESEM installation method "a wide range of tools to compose a tailored and innocent message to lure the target to open the message" and inadvertently install the Agent on the device. JA18.

Agents of the UAE, a key ally of Saudi Arabia, made six or more ESEM attempts on one of Hanan's phones in late 2017, just as she and Jamal were growing closer. JA30; JA31-32. The Emirati intelligence officers who detained Hanan at the Dubai International Airport in April 2018, *supra* at 6, also most likely manually installed Pegasus on her phones, which "takes less than five minutes," during Hanan's detention. JA15-16, JA22, JA31.

Once Pegasus is installed, Defendants play an integral part in its operation. Defendants transmit the communications and data from the target's device to their client's working station. When Pegasus captures data from the targeted device, Defendants reroute the data from the device to their Pegasus Anonymizing Transmission Network ("PATN"), which Defendants operate and maintain to protect the client, themselves, and their surveillance from detection. JA70. Defendants then route the captured data through their own servers on the way to their client's working station. JA69. Defendants map out this data transmission path for their clients as follows:

Figure 5: Data Transmission Process



JA69 (Figure 5).[2] Defendants complete these steps to make new data on the device "available *in real-time*." JA64 (emphasis added).[3]

[2] In Defendants' depiction of their spyware system, the target is a masked criminal and those spying on her are legitimate law enforcement. Undersigned counsel highlighted how, in this depiction, Hanan would be the masked criminal.

[3] *See also* Ronan Farrow, *How Democracies Spy on their Citizens*, The New Yorker (April 18, 2022) ("Farrow"), https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens ("[T]he company keeps its technology covert through an information-security department with several dozen experts. 'There is a very large department in the company which is in charge of

Defendants readily admit that they participate in obtaining the target's data. When a target starts using a new application, Defendants represent to the client that "*we can fairly easily extract the important data from virtually any application upon customer demand* and release it as a new release that will become available to the customer." JA67 (emphasis added).

More generally, one NSO Group representative explained that with Pegasus "we hear about . . . every phone call that is being hacked over the globe, we get a report immediately." JA17 (quoting Farrow, *supra*). Defendants also have remote access to the client's operating system and "can see everything that goes on," including "all of the data" they extract from a target's device. Farrow, *supra*.

Defendants also represent that they can control a client's use of the Pegasus system. They proclaim that they "shut down [their] system for customers" who misuse it. JA20-21. Defendants also represent, more specifically, that:

> NSO's Pegasus technology also has technical safeguards, such as general and customer-specific geographic limitations. One of the limitations relevant to this case is that NSO's Pegasus technology cannot be used against U.S. mobile phone numbers. *Another such limitation is that the Pegasus technology cannot be used against a device within the geographic bounds of the United States.*

---

whitewashing, I would say, all connection, all network connection between the client back to NSO,' a former employee said. 'They are purchasing servers, V.P.N. servers around the world. They have, like, this whole infrastructure set up so none of the communication can be traced.'"), article cited at JA17.

JA95 (emphasis added). Whether Defendants actually exercise these controls, however, has not been shown. *See* JA140-141 (describing reported use of Pegasus on phone number with U.S. area code; noting the absence of published analysis of a full Pegasus spyware sample since 2016). Defendants appear, in any event, to have continued monitoring and collecting data from Hanan's phones while she was in Virginia from her wedding until Jamal's execution. JA20-21, JA35.

In 2021, the U.S. Department of Commerce added NSO Group to its list of foreign entities posing a national security risk. *Addition of Certain Entities to the Entity List*, 86 Fed. Reg. 60759 (Nov. 4, 2021) (codified at 15 C.F.R. § 744). The Department found evidence that NSO Group "developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers." *Id*.

B. Procedural History

Plaintiff filed suit against Defendants in the U.S. District Court for the Eastern District of Virginia on June 15, 2023. JA7-46. She asserts claims under the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq*.; the Virginia Computer Crimes Act, Va. Code Ann. § 18.2-152.1 *et seq*. (2023); and Virginia common law. *See* JA38-44. She alleges that Defendants intentionally accessed her devices (or caused them to be accessed) without authorization, facilitated installation of the Pegasus spyware agent, and collected both existing and real-time

surveillance data from the devices, which caused her economic losses and mental and physical injuries. JA38-44. She seeks compensatory and punitive damages, equitable relief, and attorneys' fees and costs. JA45.

Defendants moved to dismiss the Complaint on six grounds: lack of subject-matter jurisdiction due to Defendants' derivative foreign sovereign immunity; lack of personal jurisdiction; the act of state doctrine; *forum non conveniens*; extraterritorial application of state law; and failure to state a claim upon which relief can be granted under Fed. R. Civ. P. 12(b)(6). *See* JA90-91; JA181 (listing arguments). Defendants filed three declarations and exhibits thereto in support of the motion, by: NSO Group CEO Yaron Shohat, JA92-129; United States-based Counsel for NSO Group, Joseph Akrotirianakis, JA130-131; and Israel-based Counsel for NSO Group, Roy Blecher, JA212-231.[4]

Plaintiff opposed the motion and filed an accompanying declaration of Bill Marczak, Senior Researcher at the Citizen Lab, JA136-142. Oral argument on the motion was held on October 20, 2023. *See* JA5-6 (Dkt. Entry 49).

The district court (Hon. Leonie M. Brinkema) granted Defendants' motion to dismiss. JA205. The court rejected Defendants' immunity arguments on subject-matter jurisdiction, but granted dismissal for lack of personal jurisdiction.

[4] To comply with foreign court orders, Defendants filed certain exhibits under seal. *See* JA232-239.

On subject-matter jurisdiction, the court rejected Defendants' argument that they were entitled to common-law foreign sovereign immunity, which deprives federal courts of jurisdiction over claims against "an individual acting in his official capacity on behalf of a foreign state." JA187-188 (quoting *Velasco v. Gov't of Indonesia*, 370 F.3d 398, 399 (4th Cir. 2004)). The court emphasized that neither Defendant is an individual or an "agency or instrumentality of a foreign state" under the Foreign Sovereign Immunity Act ("FSIA"); rather, both are privately-owned companies that are not statutorily entitled to immunity. JA188-189 (quoting 28 U.S.C. § 1603(a)). The district court cited as support *WhatsApp Inc. v. NSO Group Techs. Ltd.*, 17 F.4th 930 (9th Cir. 2021). *WhatsApp* held that "[t]here is no need to analyze whether NSO is entitled to immunity under the common law" because "[t]he proper analysis begins and ends with the FSIA, the comprehensive framework Congress enacted for resolving any entity's claim of foreign sovereign immunity." *Id.* at 940; JA188-189 (quoting *WhatsApp*). The district court also distinguished *Butters v. Vance Int'l, Inc.*, 225 F.3d 462 (4th Cir. 2000), which granted immunity to a domestic company acting in the United States under a foreign sovereign's direction, *id.* at 466, as inapposite to the foreign entity Defendants here. JA189-191.

The district court then granted dismissal under Fed. R. Civ. P. 12(b)(2), holding that it did not have personal jurisdiction over Defendants. The court noted

that Virgina's long-arm statute extends personal jurisdiction to the fullest extent the constitution permits. JA191. The court thus employed this Court's three-prong test for specific personal jurisdiction, addressing: "(1) the extent to which the defendant purposefully availed itself of the privilege of conducting activities in the State; (2) whether the plaintiffs' claims arise out of those activities directed at the State; and (3) whether the exercise of personal jurisdiction would be constitutionally reasonable." JA193 (quoting *Consulting Eng'rs Corp. v. Geometric Ltd.*, 561 F.3d 273, 278 (4th Cir. 2009)).

The district court first held that Plaintiff's allegations that Defendants targeted and surveilled her devices in Virginia were insufficient to show purposeful availment without additional allegations describing "how NSO Group specifically participated in the surveillance of her phones" and Plaintiff's whereabouts during such activities given her work as a flight attendant. JA194-195. The court also concluded that even if Plaintiff had sufficiently pled installation or data-capturing activities while she resided in Virginia, "those actions were carried out by third-parties who plaintiff alleges were using Pegasus, not by defendants." JA195.

Turning to the second prong, the court ruled that Plaintiff's allegations did not adequately link Defendants' configuration and maintenance of the Pegasus infrastructure with the conduct of its state clients; in other words, Plaintiff's allegations demonstrated infiltration of her devices "in Virginia only because of

intervening acts by third-party sovereigns." JA199-200. The court again highlighted a purported lack of allegations regarding Plaintiff's residence in Virginia amidst the relevant conduct. JA199.

On the third prong, the district court noted the five factors the Supreme Court and this Court consider in assessing constitutional reasonableness:

> (1) the burden on the defendant of litigating in the forum;
> (2) the interest of the forum state in adjudicating the dispute;
> (3) the plaintiff's interest in obtaining convenient and effective relief;
> (4) the shared interest of the states in obtaining efficient resolution of disputes; and
> (5) the interests of the states in furthering substantive social policies.

JA200 (quoting *Consulting Eng'rs*, 561 F.3d at 279). The court held that the third factor favors Plaintiff, JA201, but that the first weighs even more for Defendants, noting that they were incorporated in Israel and did not have employees, agents, evidence, or witnesses in Virginia, and that "foreign relations implications" might impair discovery. JA201. The court also presumed Israel's interest "in adjudicating conflicts concerning its corporate citizens." JA202. In holding that these interests substantially outweighed Plaintiff's (and Virginia's) interests, the district court relied on its earlier conclusion that Plaintiff did not adequately allege that Defendants committed acts in Virginia: "On balance—*factoring in plaintiff's inability to plausibly demonstrate that NSO Group directed its alleged conduct at her in Virginia*—the Court finds that exercising specific personal jurisdiction over

defendants in this district would offend constitutional due process." JA202 (emphasis added).

The district court thus granted Defendants' motion to dismiss for lack of personal jurisdiction. JA204.[5] The court dismissed all claims with prejudice, JA205, and entered judgment for Defendants. JA206.

Plaintiff filed her notice of appeal on November 21, 2023. JA207-209. Even though the district court dismissed all claims against them with prejudice, Defendants filed a notice of cross-appeal on November 28, 2023, JA210-211.

SUMMARY OF ARGUMENT

I. Virginia's long-arm statute provides that a court in Virginia may exercise jurisdiction over a person as to a cause of action arising from the person's acts in Virginia causing tortious injury. Va. Code Ann. § 8.01-328.1(A)(3) (2023). Plaintiff's allegations and claims that Defendants intentionally accessed her smartphones in Virginia without authorization and extracted and rerouted her communications and data readily satisfy these requirements. The long-arm statute separately provides that a Virginia court may exercise jurisdiction on any other basis authorized by law, Va. Code Ann. § 8.01-330 (2023), which extends jurisdiction to the extent permitted by the United States Constitution.

[5] The court also raised questions in a footnote on venue and the merits of Plaintiff's claims, JA181, but did not rule on these grounds in granting dismissal. JA204.

II. For a court to constitutionally exercise specific personal jurisdiction over claims against a defendant, the defendant must have purposefully acted in the forum state; the plaintiff's claims must relate to the defendant's in-state acts; and the exercise of jurisdiction must be reasonable. Plaintiff's claims also satisfy each of these requirements.

A. First, Defendants purposefully acted in Virginia by intentionally accessing her smartphones in Virginia without authorization and obtaining and rerouting her communications and data through their anonymizers and server to their client. These tortious acts by Defendants occurred in Virginia, where Defendants first obtained and rerouted Plaintiff's electronic information.

The district court committed two critical errors in analyzing purposeful availment. First, it held that Plaintiff did not adequately allege when and where she lived in Virginia, JA194, which ignored her specific allegations that she lived in Virginia in the four months from her marriage to Jamal on June 2, 2018, to his disappearance on October 2, 2018, and was present there during this time. JA10; JA32. Second, it held that Plaintiff did not adequately allege how Defendants participated in surveilling her devices, JA194, which ignored her showing that Defendants accessed her phones and obtained and rerouted her communications and data through their anonymizing network and server to their client. JA17, JA67, JA69-70. These are Defendants' acts in Virginia, where the devices were.

See Luis v. Zang, *supra*, 833 F.3d at 633. The district court erred in holding that Plaintiff did not adequately allege acts by Defendants in Virginia.

B. Second, Plaintiff's claims relate directly to Defendants' activity in Virginia. Defendants' acts in Virginia that Plaintiff alleges and shows are those that gave rise to her claims. *See, e.g.*, JA13-14 ("Defendants have utilized instrumentalities in Virginia (Plaintiff's personal devices) as well as targeting residents of Virginia (Hanan and Jamal Khashoggi), specifically, with knowledge that such targeting would result in significant harm to Plaintiff in Virginia . . . ."). In holding that Plaintiff did not adequately allege that her claims related to acts by Defendants in Virginia, the district court repeated the errors that underpinned its analysis of purposeful availment. JA199-200 (holding that Plaintiff failed to allege that she and Jamal lived together in Virginia after their marriage or to account for "intervening acts" by Defendants' client). The same allegations and evidence of Plaintiff's presence in Virginia and Defendants' acts in Virginia—*i.e.*, accessing her devices and obtaining and rerouting her communications and data—that undermine the district court's holding on purposeful availment likewise undermine its holding on claim-relatedness.

C. Third, the exercise of jurisdiction over Plaintiff's claims also is constitutionally reasonable for the same reasons. The district court recognized that different of the reasonableness factors favored each party. JA200-202. But in

holding that exercising jurisdiction here was not reasonable, the court relied upon its earlier conclusion that Plaintiff did not adequately allege acts by Defendants in Virginia. JA202. Since this conclusion was erroneous, so too is the ruling on constitutional reasonableness.

In light of the errors that pervaded the district court's analysis of personal jurisdiction, the order granting dismissal should be reversed.

STANDARD OF REVIEW

This Court reviews *de novo* the district court's grant of dismissal for lack of personal jurisdiction under Fed. R. Civ. P. 12(b)(2). *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344, 350 (4th Cir. 2020). Where a defendant challenges personal jurisdiction, the plaintiff has the burden of establishing jurisdiction by a preponderance of the evidence. *Id.* In determining whether the plaintiff meets its burden, the district court "may look beyond the complaint to affidavits and exhibits in order to assure itself of personal jurisdiction." *Id.* (citing *Grayson v. Anderson*, 816 F.3d 262, 269 (4th Cir. 2016)). In doing so, the district court "must . . . 'construe all relevant pleading allegations in the light most favorable to the plaintiff, assume credibility, and draw the most favorable inferences for the existence of jurisdiction.'" *Id.* (quoting *Combs v. Bakker*, 886 F.2d 673, 676 (4th Cir. 1989)).

ARGUMENT

The district court has specific personal jurisdiction over Defendants in this case. By accessing Plaintiff's smartphones in Virginia and obtaining and rerouting her communications and data through their anonymizing network and server to their client, Defendants directed electronic activity into Virginia with the manifested intent of engaging in interactions within Virginia, which gave rise to Plaintiff's causes of action. Plaintiff therefore satisfies the requirements for exercise of specific personal jurisdiction.

I. Virginia's Long-Arm Statute Covers Plaintiff's Claims.

"A federal court may exercise personal jurisdiction over a defendant in the manner provided by state law." *Young v. New Haven Advocate*, 315 F.3d 256, 261 (4th Cir. 2002). Virginia's long-arm statute provides in relevant part that a court in Virginia "may exercise personal jurisdiction over a person, who acts directly or by an agent, as to a cause of action arising from the person's . . . [c]ausing tortious injury by an act or omission in this Commonwealth[.]" Va. Code Ann. § 8.01-328.1(A)(3) (2023).

Plaintiff alleges that Defendants intentionally accessed her smartphones in Virginia and obtained and rerouted her communications and data without her authorization and that she was injured thereby while living in Virginia. JA17, JA38-39, JA40-41, JA67, JA69-70. Since Plaintiff's claims arise from these acts

by Defendants in Virginia, she readily satisfies the long-arm statute's requirements.

Virginia's long-arm statute separately provides that Virginia courts "may exercise jurisdiction on any other basis authorized by law." Va. Code Ann. § 8.01-330 (2023). This extends personal jurisdiction in Virginia's courts "to the extent permitted by the Due Process clause," so that "'the statutory inquiry necessarily merges with the constitutional inquiry, and the two inquiries essentially become one.'" *Young*, 315 F.3d at 261 (quoting *Stover v. O'Connell Assocs., Inc.*, 84 F.3d 132, 135-36 (4th Cir. 1996)). Since Plaintiff also satisfies the constitutional requirements for specific personal jurisdiction, as set forth below, she satisfies the state-law requirements for jurisdiction set forth in Virginia's long-arm statute.

II. Plaintiff Satisfies the Constitutional Requirements for Specific Personal Jurisdiction.

A court's constitutional authority to exercise jurisdiction over a defendant "depends on the defendant's having such 'contacts' with the forum State that 'the maintenance of the suit' is 'reasonable in the context of our federal system of government,' and 'does not offend traditional notions of fair play and substantial justice.'" *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.*, 592 U.S. 351, 358 (2021) (quoting *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316-17 (1945)). The constitutional inquiry thus focuses on "the nature and extent of 'the defendant's relationship to the forum State.'" *Id.* (quoting *Bristol-Myers Squibb Co. v.*

Superior Ct. of Cal., 582 U.S. 255, 262 (2017)). This focus, in turn, has led courts to recognize "two kinds of personal jurisdiction: general (sometimes called all-purpose) jurisdiction and specific (sometimes called case-linked) jurisdiction." *Id.*

The first, general jurisdiction, "extends to 'any and all claims' brought against a defendant[,]" *id.* (quoting *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 919 (2011)), but applies only to a select set of contacts or affiliations of the defendant. *Id.* The paradigm forums for exercising general jurisdiction over a corporate defendant are "its place of incorporation and principal place of business." *Id.* at 358-59. Here, Defendants are incorporated and headquartered outside of Virginia, in Israel. JA11. Plaintiff thus does not contend that there is general personal jurisdiction over Defendants in Virginia.

Instead, this appeal turns on the second type of constitutional exercise of personal jurisdiction—specific or case-linked jurisdiction. Specific jurisdiction "covers defendants less intimately connected with a State, but only as to a narrower class of claims." *Ford Motor*, 592 U.S. at 359. For a court to exercise specific personal jurisdiction, three requirements must be satisfied. First, the defendant "must take 'some act by which [it] purposefully avails itself of the privilege of conducting activities within the forum State.'" *Id.* (quoting *Hanson v. Denckla*, 357 U.S. 235, 253 (1958)). Second, "the plaintiff's claims . . . 'must arise out of or relate to the defendant's contacts' with the forum." *Id.* (quoting

Bristol-Myers Squibb, 582 U.S. at 262). Third, the exercise of personal jurisdiction must be "constitutionally reasonable." *Consulting Eng'rs*, 561 F.3d at 278. Here, Plaintiff satisfies each of these requirements for specific personal jurisdiction.

A. Defendants Purposefully Committed Acts in Virginia.

Plaintiff alleges and demonstrates that Defendants purposefully committed acts in Virginia. *First*, Defendants intentionally accessed her smartphones in Virginia without authorization. JA17 (NSO Group "hear[s] about . . . every phone call that is being hacked over the globe, [and] get[s] a report immediately," and offers "data acquisition, and analysis"); JA38-39, JA40-41. *Second*, Defendants obtained her communications and data from her phones and rerouted this information through their anonymizing transmission network to conceal their surveillance. JA67 ("[W]e can fairly easily extract the important data from virtually any application upon customer demand . . . ."); JA69 (Figure 5: "Data Transmission Process" from target's device to Defendants' Anonymizers); JA70 ("[T]he Pegasus Anonymizing Transmission Network, a network of anonymizers[,] is deployed to serve each customer."). *Third*, Defendants transmitted the information through their data server to their client—the United Arab Emirates. JA69 (Figure 5). Defendants' acts of accessing Plaintiff's devices in Virginia and obtaining and rerouting her communications and data satisfy the constitutional requirement of purposeful activity in the forum state.

Case law on purposeful availment makes clear that Defendants' acts in Virginia from which Plaintiff's claims arise support specific personal jurisdiction. A defendant's act or acts connected with the forum state "must be [by] the defendant's own choice and not 'random, isolated, or fortuitous.'" *Ford Motor*, 592 U.S. at 359 (quoting *Keeton v. Hustler Magazine, Inc.*, 465 U.S. 770, 774 (1984)). However, "even a single act can support jurisdiction" if it "creates a 'substantial connection' with the forum[.]" *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 n.18 (1985) (quoting *McGee v. Int'l Life Ins. Co.*, 355 U.S. 220, 223 (1957)); *see also Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc.*, 334 F.3d 390, 397 (4th Cir. 2003) ("Even a single contact may be sufficient to create jurisdiction when the cause of action arises out of that single contact, provided that the principle of 'fair play and substantial justice' is not thereby offended.") (quoting *Burger King*, 471 U.S. at 477-78).

Where, as here, a defendant's contacts arise from its electronic activity rather than its physical presence in the forum state, this Court assesses the defendant's activity and forum contacts as follows:

> [W]e conclude that a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts.

ALS Scan, Inc. v. Digital Service Consultants, Inc., 293 F.3d 707, 714 (4th Cir. 2002). Here, too, a "single act" of electronic activity by the defendant may suffice to establish jurisdiction. *Automobili Lamborghini S.P.A. v. Lamborghini Latino Am. USA*, 400 F. Supp. 3d 471, 474 (E.D. Va. 2019).

Here, Defendants' acts of electronically accessing Plaintiff's smartphones in Virginia without authorization and obtaining and rerouting her communications and data over the course of four months satisfy the constitutional forum contacts requirement for specific personal jurisdiction.

In holding to the contrary, the district court misapprehended two key points. First, it held that "the Complaint fails to include any non-conclusory allegations regarding how long and where plaintiff had been living in the district[.]" JA194. This is incorrect. The Complaint specifically alleges that Plaintiff lived at her and Jamal's marital home in Virginia from June 2, 2018 (their marriage) to and beyond October 2, 2018 (Jamal's disappearance) and was present there during some (though not all) of this period. JA10 ("In June 2018, the couple was married . . . in Virginia. After their wedding, the newlyweds lived in their shared Tysons Corner, Virginia condominium as husband and wife."); JA32 (Hanan and Jamal "spent the next weeks moving into and decorating their shared apartment in Virginia and making it their home."); JA32 ("Although Hanan's job as a flight attendant kept her traveling often, anytime she was able to be, she was home with Jamal.").

Plaintiff thus alleges that she and her devices that Defendants accessed were in Virginia during this time.

Moreover, to the extent the district court inferred that Defendants accessed Plaintiff's phones only when she was outside Virginia, *see* JA194 (referencing "conduct that *may have* happened while she was overseas or traveling for work as a flight attendant for Emirates Airlines.") (emphasis added), this inference *against* Plaintiff is improper. *UMG Recordings*, 963 F.3d at 350 (plaintiff must receive all favorable inferences on Rule 12(b)(2) motion).

Second, the district court held that "the Complaint fails to include any non-conclusory allegations regarding . . . how NSO Group specifically participated in the surveillance of [Plaintiff's] phones . . ." and does not "allege facts that counter defendants' argument that the non-party Saudi and Emirati governments were the ones using the Pegasus technology to surveil plaintiff." JA194; *see also* JA195 ("[T]hose actions were carried out by third-parties who plaintiff alleges were using Pegasus, not by defendants."). This, too, is plainly incorrect.

The Complaint and its Exhibit—Defendants' own "Pegasus – Product Description"—make clear that Defendants themselves:

- access the devices, communications, and data that their clients target; JA17 ("[W]e hear about . . . every phone call that is being hacked over the globe, we get a report immediately.") (quoting employee interview in Farrow, *supra*); JA17 (NSO Group offers its clients "cyber intelligence, data acquisition, *and analysis*") (quoting *2019 ISS World Europe -Lead Sponsor*, TeleStrategies ISS World Europe

[https://web.archive.org/web/20190908051829/https://www.issworldtraining.com/iss_europe/sponsors.html] (last visited Mar. 29, 2024)) (emphasis added);

- obtain or extract the target's communications and data; JA67 ("[W]e can fairly easily extract the important data from virtually any application upon customer demand and release it as a new release that will become available to the customer.");

- anonymize their access and extraction to prevent detection; JA70 ("To assure that trace back to the operating organization is impossible, the Pegasus Anonymizing Transmission Network (PATN), a network of anonymizers is deployed to serve each customer. The PATN nodes are spread in different locations around the world, allowing agent connections to be redirected through different paths prior to reaching the Pegasus servers. This ensures that the identities of both communicating parties are highly obscured."); and

- reroute the extracted information from the target's device through the anonymizing network and the "Pegasus Data Server" to the client's working station; JA69 (Figure 5: Data Transmission Process).

The district court thus erred in holding that Plaintiff alleges no facts showing that Defendants acted in Virginia, where Plaintiff and her phones were.

The district court's misapprehension as to Defendants' activity in accessing Plaintiff's devices and obtaining and rerouting her information is critical. This led the court to ignore authority holding that the place where unlawful interception of electronic data occurs is where the data is *first captured and rerouted*. In *Popa v. Harriet Carter Gifts, Inc.*, *supra*, the Third Circuit addressed a Pennsylvania consumer's claim that an online retailer (Harriet Carter) and its third-party marketing service (NaviStone) unlawfully tracked her activity across the retailer's

website. 52 F.4th at 124. In analyzing where the interception of the plaintiff's data took place, the court held that it occurred on the plaintiff's browser where the defendant first obtained and rerouted the data to its own servers. *Id.* at 131 ("NaviStone intercepted Popa's communications at the point where it routed those communications to its own servers. *And that was at Popa's browser, not where the signals were received at NaviStone's servers.*") (emphasis added).

In *Luis v. Zang*, *supra*, the Sixth Circuit likewise held that the unlawful capture of electronic communications occurs where spyware accesses the communication and reroutes it to another's server. 833 F.3d at 633. There, the court addressed claims by a plaintiff whose online communications were intercepted by spyware ("WebWatcher") manufactured and operated by defendant Awareness Technologies and installed by defendant Zang on his wife's computer, to which the plaintiff was communicating. *Id.* at 623. The Sixth Circuit, like the Third Circuit in *Popa*, held that the "alleged intercept of a communication . . . occurs at the point where WebWatcher—without any active input from the user—captures the communication and reroutes it to Awareness's own servers." *Id.* at 633. The Third and Sixth Circuits' focus on the place where data is first captured and rerouted thus supports Plaintiff's argument herein that her communications and data were unlawfully obtained where she and her devices were, in Virginia.

The Sixth Circuit's decision also supports Plaintiff's claim that Defendants themselves accessed her devices and obtained her information. In *Luis*, as here, the spyware company tried to avoid liability by blaming its client who selected the device to be surveilled. The Sixth Circuit rejected this argument, holding that the spyware company itself participated in obtaining his communications:

> Where the district court erred was in failing to recognize that Luis alleges *not only that Awareness manufactures and sells WebWatcher, but that, once installed on a computer, WebWatcher automatically acquires and transmits communications to servers that Awareness owns and maintains*. . . . [T]he complaint supports an inference that Awareness itself—not simply the WebWatcher user—'acquires' the communications by rerouting them to servers that it owns and controls. That, in turn, suggests that awareness itself is responsible for the alleged intercept.

Luis, 833 F.3d at 633 (emphasis added). In holding both (1) that interception of electronic information occurs where it is first accessed and rerouted, and (2) that a spyware company's unauthorized interception and rerouting of a target's electronic information through its own servers to its client is tortious conduct, the Sixth Circuit's decision strongly supports a holding here that Plaintiff alleges purposeful and tortious acts by Defendants in Virginia.

Since the district court erred in holding that there is no allegation or evidence of Plaintiff's presence or Defendants' acts in Virginia, its holding that Defendants did not have sufficient forum contacts was likewise erroneous and should be reversed.

B. Plaintiff's Claims Relate Directly to Defendants' Acts in Virginia.

Once Defendants' purposeful activity in Virginia is established, the relationship between these acts and Plaintiff's claims is clear and direct and readily supports exercise of specific personal jurisdiction.

The Supreme Court long has held that a foreign defendant may be called to respond to a suit relating to its purposeful acts in the forum jurisdiction. In its foundational *International Shoe* opinion, the Court explained the fundamental fairness of this exercise of jurisdiction as follows:

> [T]o the extent that a corporation exercises the privilege of conducting activities within a state, it enjoys the benefits and protection of the laws of that state. The exercise of that privilege may give rise to obligations; and, so far as those obligations arise out of or are connected with the activities within the state, a procedure which requires the corporation to respond to a suit brought to enforce them can, in most instances, hardly be said to be undue.

326 U.S. at 319. In light of this recognition, "for a state court to exercise specific jurisdiction, 'the *suit*' must 'arise out of or relate to the defendant's contacts with the *forum*.'" *Bristol-Myers Squibb*, 582 U.S. at 262 (quoting *Daimler AG v. Bauman*, 571 U.S. 117, 127 (2014)) (emphasis in citing opinion). The relationship or affiliation between the suit and the forum can, but need not be, causal in nature. *Ford Motor*, 592 U.S. at 362 ("[W]e have never framed the specific jurisdiction inquiry as always requiring proof of causation—*i.e.*, proof that the plaintiff's claim came about because of the defendant's in-state conduct.").

Here, Defendants' acts in Virginia relate directly and give rise to Plaintiff's claims. *See, e.g.*, JA12 (Defendants "intentionally target[ed] Hanan (and through Hanan, Jamal) and her devices in Virginia"); JA13-14 ("Defendants have utilized instrumentalities located in Virginia (Plaintiff's personal devices) as well as targeting residents of Virginia (Hanan and Jamal Khashoggi), specifically with knowledge that such targeting would result in significant harm to Plaintiff in Virginia . . . ."); JA14 ("Defendants expressly aimed their tortious conduct at the Plaintiff in Virginia such that Virginia can be said to be the focal point of the tortious activity."); JA35 ("Defendants and their clients were aware that Jamal and Hanan were living together in Virginia and that Hanan has continued to reside in Virginia, where she was monitored . . . .").

In holding that Plaintiff "has not adequately alleged that her claims arose out of conduct defendants directed at and conducted in Virginia[,]" JA200, the district court again misapprehended Plaintiff's allegations as to both her residence in Virginia and Defendants' participation in accessing and obtaining information from her smartphones in Virginia.

First, the district court erroneously held that Plaintiff's allegation that she resided in Virginia after she and Jamal were married was a "newly postulated" fact raised for the first time at oral argument. JA199. This again is plainly incorrect. The Complaint specifically alleges that Plaintiff lived and spent time in Virgina

between her marriage to Jamal on June 2, 2018, and his disappearance on October 2, 2018. JA10 ("In June 2018, the couple was married by an Imam in an Islamic ceremony in Virginia. After their wedding, the newlyweds lived in their shared Tysons Corner, Virginia condominium as husband and wife."); JA32 (after their June 2, 2018 wedding, Hanan and Jamal "spent the next weeks moving into and decorating their shared apartment in Virginia and making it their home."); JA32 ("Although Hanan's job as a flight attendant kept her traveling often, anytime she was able to be, she was home with Jamal.").

Second, the district court also erred in holding that Plaintiff "at best . . . pleaded that NSO Group's Pegasus technology infiltrated her devices in Virginia only because of intervening acts by third-party sovereigns." JA199. As set forth, *supra* at 26-27, Plaintiff alleges and shows that Defendants themselves access the devices that their clients target, JA17; obtain the target's communications and data, JA67; anonymize their activity to prevent detection, JA70; and reroute the information from the target's device through their anonymizing network and "Pegasus Data Server" to the client's working station, JA69 (Figure 5).

Addressing nearly identical allegations, the Sixth Circuit held that these acts make the spyware manufacturer-operator a participant with its client in unlawfully obtaining information from a computer. *Luis v. Zang*, 833 F.3d at 633 (allegation that Awareness (WebWatcher manufacturer) "acquires and transmits

communications to servers that Awareness owns and maintains . . . supports an inference that Awareness itself—not simply the WebWatcher user—'aquires' the communications by rerouting them to servers that it owns and controls").[6]

This Court should hold the same and should reverse the district court's erroneous holding that there is no allegation or evidence connecting Plaintiff's claims to acts by Defendants in Virginia.

C. This Exercise of Personal Jurisdiction is Constitutionally Reasonable.

The district court's exercise of personal jurisdiction over Plaintiff's claims against Defendants based on their accessing and extracting information from her devices in Virginia is constitutionally reasonable. In assessing the reasonableness of exercising personal jurisdiction, courts consider:

> (1) the burden on the defendant of litigating in the forum; (2) the interest of the forum state in adjudicating the dispute; (3) the plaintiff's interest in obtaining convenient and effective relief; (4) the

[6] The unpublished opinion that the district court relied on for its "intervening acts" holding is materially different. In *St. Jarre v. Heidelberger Druckmaschinen, A.G.*, 19 F.3d 1430 (4th Cir. Mar. 25, 1994) (unpub.), this Court held that there was no personal jurisdiction over claims against a foreign manufacturer for product-related injuries that occurred 15 years and four sales after the manufacturer relinquished the product. *See id.* at *1 ("The printing press that allegedly caused the accident was sold by HDAG to Heidelberg Eastern fifteen years before the accident. Heidelberg Eastern sold the press to a company in Michigan and it was later sold to a company in New Mexico. The company in New Mexico then sold the press to St. Jarre's employer in Norfolk, Virginia."). This is a far cry from Plaintiff's allegations and evidence here that she was harmed from Defendants' own operation of their spyware system on her phones in Virginia.

> shared interest of the states in obtaining efficient resolution of disputes; and (5) the interests of the states in furthering substantive social policies.

Consulting Eng'rs, 561 F.3d at 279.

Where, as here, the requirements for personal jurisdiction are otherwise satisfied, the burden shifts to the defendant to "present a compelling case that the presence of some other considerations would render jurisdiction unreasonable." *Burger King*, 471 U.S. at 477. A defendant does not carry this substantial burden when the reasonableness factors are in or near equipoise. *Harris Rutsky & Co. Ins. Servs., Inc. v. Bell & Clements Ltd.*, 328 F.3d 1122, 1134 (9th Cir. 2003) (where "some of the reasonableness factors weigh in favor of [defendant], but others weigh against it," the defendant "has not met its burden of presenting a compelling case that the exercise of jurisdiction would not comport with fair play and substantial justice.").

Here, the party and forum interests do not clearly favor Defendants, so that personal jurisdiction is constitutionally reasonable. The second and third factors (forum state's and Plaintiff's interests) favor exercise of personal jurisdiction, *see* JA201 (finding third factor to favor Plaintiff), while the first (Defendants' burden) weighs against, and the fourth and fifth (interests in efficient resolution and furthering substantive policies) weigh no more for Defendants than for Plaintiff.

Thus, Defendants do not satisfy their burden of making a compelling case that personal jurisdiction is unreasonable.

In *WhatsApp Inc. v. NSO Group Techs. Ltd.*, 472 F. Supp. 3d 649 (N.D. Cal. 2020), the court applied similar reasonableness factors in holding that it had personal jurisdiction over a United States plaintiff's claims against NSO Group and Q Cyber. In *WhatsApp*, the plaintiff alleged that NSO Group and Q Cyber "sent malware, using WhatsApp's system, to approximately 1,400 mobile phones and devices designed to infect those devices for the purpose of surveilling the users of those phones and devices." *Id.* at 658. There, like here, NSO Group and Q Cyber defended by alleging that "the conduct giving rise to the complaint was performed by foreign sovereigns[.]" *Id.* at 663. The court held, however, that WhatsApp sufficiently alleged that NSO Group and Q Cyber purposefully directed tortious acts into the United States from which its claims arose. *Id.* at 669-74.

In analyzing constitutional reasonableness, the *WhatsApp* court found that the respective party and sovereign interests at issue were roughly in balance. *Id.* at 676-77 ("In sum, some factors tip in defendants' favor and other factors tip in plaintiffs' favor."). The court thus held that the "defendant has not carried its burden to present a compelling case that exercising jurisdiction would be unreasonable." *Id.* at 677. The same conclusion should apply here.

In holding to the contrary, that personal jurisdiction over the same defendants for the same type of acts in the United States was constitutionally *unreasonable*, the district court below again relied on its erroneous conclusion that Defendants did not direct electronic activity into Virginia. After holding that the reasonableness factors pointed in different directions, JA200-202, the court concluded as follows:

> On balance—*factoring in plaintiff's inability to plausibly demonstrate that NSO Group directed its alleged conduct at her in Virginia*—the Court finds that exercising specific personal jurisdiction over defendants in this district would offend constitutional due process.

JA202 (emphasis added). Since, as shown above, the district court erred when it held that Defendants did not commit acts in Virginia, it likewise erred in holding that personal jurisdiction is constitutionally unreasonable.

For all of the reasons set forth, the district court's holding that it lacked personal jurisdiction over Plaintiff's claims arising from Defendants' purposeful acts in Virginia was erroneous and should be reversed.

CONCLUSION

The district court's judgment should be reversed.

REQUEST FOR ORAL ARGUMENT

Because this appeal involves complex issues of law and alleged fact, Appellant/Cross-Appellee respectfully requests oral argument.

Respectfully submitted,

/s/ *Michael J. Quirk*

Michael J. Pendell
MOTLEY RICE LLC
One Corporate Center
20 Church Street, 17th Floor
Hartford, CT 06103
(860) 882-1681
mpendell@motleyrice.com

Michael J. Quirk
MOTLEY RICE LLC
40 West Evergreen Avenue,
Suite 104
Philadelphia, PA 19118-3324
(610) 579-9932
mquirk@motleyrice.com

Counsel for Plaintiff-Appellant/Cross-Appellee
Hanan Elatr Khashoggi

April 1, 2024

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

Nos. 23-2234(L) & 23-2241 Caption: Hanan Elatr Khashoggi v. NSO Grp. Techn. et al.

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT

Type-Volume Limit, Typeface Requirements, and Type-Style Requirements

Type-Volume Limit for Briefs if Produced Using a Computer: Appellant's Opening Brief, Appellee's Response Brief, and Appellant's Response/Reply Brief may not exceed 13,000 words or 1,300 lines. Appellee's Opening/Response Brief may not exceed 15,300 words or 1,500 lines. A Reply or Amicus Brief may not exceed 6,500 words or 650 lines. Amicus Brief in support of an Opening/Response Brief may not exceed 7,650 words. Amicus Brief filed during consideration of petition for rehearing may not exceed 2,600 words. Counsel may rely on the word or line count of the word-processing program used to prepare the document. The word-processing program must be set to include headings, footnotes, and quotes in the count. Line count is used only with monospaced type. See Fed. R. App. P. 28.1(e), 29(a)(5), 32(a)(7)(B) & 32(f).

Type-Volume Limit for Other Documents if Produced Using a Computer: Petition for permission to appeal and a motion or response thereto may not exceed 5,200 words. Reply to a motion may not exceed 2,600 words. Petition for writ of mandamus or prohibition or other extraordinary writ may not exceed 7,800 words. Petition for rehearing or rehearing en banc may not exceed 3,900 words. Fed. R. App. P. 5(c)(1), 21(d), 27(d)(2), 35(d)(2) & 40(b)(1).

Typeface and Type Style Requirements: A proportionally spaced typeface (such as Times New Roman) must include serifs and must be 14-point or larger. A monospaced typeface (such as Courier New) must be 12-point or larger (at least 10½ characters per inch). Fed. R. App. P. 32(a)(5), 32(a)(6).

This brief or other document complies with type-volume limits because, excluding the parts of the document exempted by Fed. R. App. P. 32(f) (cover page, disclosure statement, table of contents, table of citations, statement regarding oral argument, signature block, certificates of counsel, addendum, attachments):

X this brief or other document contains **8,231** words

n.a. this brief uses monospaced type and contains _____ lines

This brief or other document complies with the typeface and type style requirements because:

X this brief or other document has been prepared in a proportionally spaced typeface using Microsoft Office Word 2016 in Times New Roman 14.

/s/ *Michael J. Quirk*
Party Name: Hanan Elatr Khashoggi
Dated: April 1, 2024

CERTIFICATE OF SERVICE

I hereby certify that, on April 1, 2024, I electronically filed the foregoing Brief for Appellant with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

/s/ *Michael J. Quirk*
Michael J. Quirk